

Australian Standard™

**Electronic funds transfer—
Requirements for interfaces**

**Part 6.3: Key management—
Session keys—Node to node**

This Australian Standard was prepared by Committee IT-005, Financial Transaction Systems. It was approved on behalf of the Council of Standards Australia on 16 June 2000 and published on 11 September 2000.

The following are represented on Committee IT-005:

Australian Association of Permanent Building Societies
Australian Bankers Association
Australian Electrical and Electronic Manufacturers Association
Australian Institute of Petroleum
Australian Retailers Association
Consumers Federation of Australia
Credit Card Industry
Credit Union Services Corporation (Australia)
Department of Defence, Australia
Independent EFT Services
Reserve Bank of Australia
Telstra Corporation

Keeping Standards up-to-date

Standards are living documents which reflect progress in science, technology and systems. To maintain their currency, all Standards are periodically reviewed, and new editions are published. Between editions, amendments may be issued. Standards may also be withdrawn. It is important that readers assure themselves they are using a current Standard, which should include any amendments which may have been published since the Standard was purchased.

Detailed information about Standards can be found by visiting the Standards Australia web site at www.standards.com.au and looking up the relevant Standard in the on-line catalogue.

Alternatively, the printed Catalogue provides information current at 1 January each year, and the monthly magazine, *The Australian Standard*, has a full listing of revisions and amendments published each month.

We also welcome suggestions for improvement in our Standards, and especially encourage readers to notify us immediately of any apparent inaccuracies or ambiguities. Contact us via email at mail@standards.com.au, or write to the Chief Executive, Standards Australia International Ltd, GPO Box 5420, Sydney, NSW 2001.

Australian Standard™

**Electronic funds transfer—
Requirements for interfaces**

**Part 6.3: Key management—
Session keys—Node to node**

Originated as AS 2805.6.3—1998.
Second edition 2000.
Reissued incorporating Amendment No. 1 (March 2003).

COPYRIGHT

© Standards Australia International

All rights are reserved. No part of this work may be reproduced or copied in any form or by any means, electronic or mechanical, including photocopying, without the written permission of the publisher.

Published by Standards Australia International Ltd
GPO Box 5420, Sydney, NSW 2001, Australia

ISBN 0 7337 3511 8

PREFACE

This Standard was prepared by the Standards Australia Committee IT-005, Financial Transaction Systems, to supersede AS 2805.6.3—1998.

This Standard incorporates Amendment No. 1 (March 2003). The changes required by the Amendment are indicated in the text by a marginal bar and amendment number against the clause, note, table, figure or part thereof affected.

This Standard is Part 6.3 of the following series:

AS

2805	Electronic funds transfer—Requirements for interfaces
2805.1	Part 1: Communications
2805.2	Part 2: Message structure, format and content
2805.3	Part 3: PIN management and security
2805.4	Part 4: Message authentication
2805.5.1	Part 5.1: Ciphers—Data encipherment algorithm 1 (DEA 1)
2805.5.2	Part 5.2: Ciphers—Modes of operation for an n-bit block cipher algorithm
2805.5.3	Part 5.3: Ciphers—Data encipherment algorithm 2 (DEA 2)
2805.5.4	Part 5.4: Ciphers—Data encipherment algorithm 3 (DEA 3) and related techniques
2805.6.1	Part 6.1: Key management—Principles
2805.6.2	Part 6.2: Key management—Transaction keys
2805.6.3	Part 6.3: Key management—Session keys—Node to node (this Standard)
2805.6.4	Part 6.4: Key management—Session keys—Terminal to acquirer
2805.6.5.1	Part 6.5.1: Key management—TCU initialization—Principles
2805.6.5.2	Part 6.5.2: Key management—TCU initialization—Symmetric
2805.6.5.3	Part 6.5.3: Key management—TCU initialization—Asymmetric
2805.9	Part 9: Privacy of communications
2805.10	Part 10: File transfer integrity validation
2805.11	Part 11: Card parameter table
2805.12.1	Part 12.1: Message content—Structure and format
2805.12.2	Part 12.2: Message content—Codes
2805.12.3	Part 12.3: Message content—Maintenance of codes
2805.13.1	Part 13.1: Secure hash functions—General
2805.13.2	Part 13.2: Secure hash functions—MD5
2805.13.3	Part 13.3: Secure hash functions—SHA-1
2805.14.1	Part 14.1: Secure cryptographic devices (retail)—Concepts, requirements and evaluation methods

The following Handbooks relate to AS 2805 series of Standards:

HB 127	Electronic funds transfer—Implementing message content Standards—Conversion Handbook (changing from AS 2805.2 to AS 2805.12 series)
HB 128	Electronic funds transfer—Implementing message content Standards—Terminal Handbook
HB 129	Electronic funds transfer—Implementing message content Standards—Interchange Handbook

Part of the AS 2805 series that is in the course of preparation is as follows:

Message authentication using DEA 3.

In the AS 2805 series of Standards, the definitions of words and phrases used are specific to the Part in which they appear.

The term ‘normative’ has been used in this Standard to define the application of the appendix to which it applies. A ‘normative’ appendix is an integral part of a Standard.

CONTENTS

	<i>Page</i>
1 SCOPE	4
2 APPLICATION	4
3 REFERENCED DOCUMENTS	4
4 DEFINITIONS	5
5 OVERVIEW	9
6 DESCRIPTION OF FUNCTIONAL ELEMENTS	9
7 OPERATION	10
APPENDICES	
A NOTATION	13
B INITIALIZATION SCHEMES	16

Australian Standard
Electronic funds transfer—Requirements for interfaces

Part 6.3: Key management—Session keys—Node to node

1 SCOPE

This Standard specifies management techniques for keys used in the authentication, encipherment and decipherment of electronic messages relating to financial transactions using session keys.

In particular, this Standard—

- (a) defines security interface procedures between nodes;
- (b) defines methods of interchange of the various encipherment keys used for securing transactions; and
- (c) ensures that messages can only be authenticated at their correct destination.

NOTE: Principles concerning key management and physical security are dealt with in AS 2805.6.1.

2 APPLICATION

This Standard may be adopted in all situations where a secure node-to-node dialogue is desired.

3 REFERENCED DOCUMENTS

The following documents are referred to in this Standard:

AS

2805	Electronic funds transfer—Requirements for interfaces
2805.2	Part 2: Message structure, format and content
2805.3	Part 3: PIN management and security
2805.4	Part 4: Message authentication
2805.5.1	Part 5.1: Ciphers—Data encipherment algorithm 1 (DEA 1)
2805.5.3	Part 5.3: Ciphers—Data encipherment algorithm 2 (DEA 2)
2805.5.4	Part 5.4: Ciphers—Data encipherment algorithm 3 (DEA 3) and related techniques
2805.6.1	Part 6.1: Key management—Principles
2805.6.2	Part 6.2: Key management—Transaction keys
2805.6.4	Part 6.4: Key management—Session keys—Terminal to acquirer
2805.13.1	Part 13.1: Secure hash functions—General
2805.13.2	Part 13.2: Secure hash functions—MD5
2805.14.1	Part 14.1: Secure cryptographic devices (retail)—Concepts, requirements and evaluation methods
3620	Information processing systems—Open Systems Interconnection—Service conventions